IN THE CLAIMS:

1. (Currently amended) A computer-implemented method of generating a security object for use in authenticating a user to access ~~securing~~ an item, comprising computer-implemented steps of:

receiving security object data;

setting one or more attributes associated with the security object data, wherein the one or more attributes include a user designation of a security object type; and

encapsulating, within the security object, the security object data and the one or more attributes with one or more methods, wherein the security object is used to authenticate the user by validating an identity of the user using at least one of the one or more methods encapsulated within the security object ~~control access to secured contents~~.

2. (Currently amended) The computer-implemented method of claim 1, further comprising obtaining the one or more methods from a security object class.

3. (Currently amended) The computer-implemented method of claim 1, wherein the one or more methods operate on the security object data and one or more attributes.

4. (Currently amended) The computer-implemented method of claim 1, wherein the one or more methods operate on the security object data and input data provided by the user and passed to the security object to authenticate the user to access the item.

5. (Currently amended) The computer-implemented method of claim 1, wherein the security object data is one of textual data, audio data, graphical data, and biometric data.

6. (Currently amended) The computer-implemented method of claim 1, wherein the security object type is one of a single use security object, a group security object, a timed security object, a concurrent multi-user security object, a security object throttle, a translated password security object, a security object augmented by a at least one of a CPU identifier, a CPU speed and a system configuration, a Wave file or MP3 security

object, an image file security object, a security object augmented by a location of the user, a security object augmented by a current window and/or pointer position, a security object augmented by an IP address, a security object augmented by a screen background characteristic, a security object augmented by a personal identification number one of a speed of a card swipe and a number of times of a card swipe, a security object augmented by a mobile telephone ring or mobile telephone identification number, a security object augmented by a caller identification of the user, and a security object augmented by an environmental condition.

7. (Currently amended) The computer-implemented method of claim 1, further comprising:

providing the security object to a security system, wherein the security system is ~~not made aware of the security object type~~ a hardware data processing system that stores the security object and associates the security object with a user identification so that the security object may be retrieved when the user enters their identification in order to gain access to the item.

8. (Currently amended) The computer-implemented method of claim 7, wherein the security system invokes the security object in response to a request for access to the item by the user.

9. (Currently amended) The computer-implemented method of claim 1, storing the security object data on an electronic medium in a device with data transmission capability.

10. (Currently amended) The computer-implemented method of claim 9, wherein the device is a portable device.

11. (Currently amended) The computer-implemented method of claim 9, wherein the portable device is one of a keychain, a portable MP3 player, a mobile telephone, a pager,

an electronic wrist watch, a remote control, a garage door transmitter, a keyless entry device for a vehicle, a smartcard, and a magnetic stripe card.

12. (Currently amended) The computer-implemented method of claim 7, wherein the security object contains a partial set of methods and wherein the security system contains a complementary set of methods.

13. (Currently amended) The computer-implemented method of claim 1, wherein the security object requires hardware assistance for authentication of input data passed to the security object.

14. (Currently amended) The computer-implemented method of claim 1, wherein the security object data is received from a client apparatus.

15. (Currently amended) The computer-implemented method of claim 1, wherein the security object data is received from a user via a user interface.

16. (Currently amended) The computer-implemented method of claim 15, wherein the user interface is a security object foundry application resident on a computing device.

17. (Currently amended) The computer-implemented method of claim 15, wherein the user interface is an interface transmitted from a server apparatus to a client apparatus.

18. (Currently amended) A computer program product in a computer readable medium for generating a security object for use in authenticating a user to access ~~securing~~ an item, comprising:

first instructions for receiving security object data;

second instructions for setting one or more attributes associated with the security object data, wherein the one or more attributes include a user designation of a security object type; and

third instructions for encapsulating, within the security object, the security object data and the one or more attributes with one or more methods, wherein the security object is used to authenticate the user by validating an identity of the user using at least one of the one or more methods encapsulated within the security object ~~control access to secured contents~~.

19. (Original) The computer program product of claim 18, fourth instructions for obtaining the one or more methods from a security object class.

20. (Original) The computer program product of claim 18, wherein the one or more methods operate on the security object data and one or more attributes.

21. (Currently amended) The computer program product of claim 18, wherein the one or more methods operate on the security object data and input data provided by the user and passed to the security object to authenticate the user to access the item.

22. (Original) The computer program product of claim 18, wherein the security object data is one of textual data, audio data, graphical data, and biometric data.

23. (Original) The computer program product of claim 18, wherein the security object type is one of a single use security object, a group security object, a timed security object, a concurrent multi-user security object, a security object throttle, a translated password security object, a security object augmented by a at least one of a CPU identifier, a CPU speed and a system configuration, a Wave file or MP3 security object, an image file security object, a security object augmented by a location of the user, a security object augmented by a current window and/or pointer position, a security object augmented by an IP address, a security object augmented by a screen background characteristic, a security object augmented by a personal identification number and one of a speed of a card swipe and a number of times of a card swipe, a security object augmented by a mobile telephone ring or mobile telephone identification number, a

security object augmented by a caller identification of the user, and a security object augmented by an environmental condition.

24. (Currently amended) The computer program product of claim 18, further comprising:

fourth instructions for providing the security object to a security system, wherein the security system is ~~not made aware of the security object type~~ a hardware data processing system that stores the security object and associates the security object with a user identification so that the security object may be retrieved when the user enters their identification in order to gain access to the item.

25. (Currently amended) The computer program product of claim 24, wherein the security system invokes the security object in response to a request for access to the item by the user.

26. (Original) The computer program product of claim 18, further comprising fourth instructions for storing the security object data on an electronic medium in a device with data transmission capability.

27. (Original) The computer program product of claim 18, further comprising fourth instructions for storing the security object data in a portable device.

28. (Original) The computer program product of claim 27, wherein the portable device is one of a keychain, a portable MP3 player, a mobile telephone, a pager, an electronic wrist watch, a remote control, a garage door transmitter, a keyless entry device for a vehicle, a smartcard, and a magnetic stripe card.

29. (Original) The computer program product of claim 24, wherein the security object contains a partial set of methods and wherein the security system contains a complementary set of methods.

30. (Original) The computer program product of claim 18, wherein the security object requires hardware assistance for authentication of input data passed to the security object.

31. (Original) The computer program product of claim 18, wherein the security object data is received from a client apparatus.

32. (Original) The computer program product of claim 18, wherein the security object data is received from a user via a user interface.

33. (Original) The computer program product of claim 32, wherein the user interface is a security object foundry application resident on a computing device.

34. (Original) The computer program product of claim 32, wherein the user interface is an interface transmitted from a server apparatus to a client apparatus.

35. (Currently amended) An apparatus for generating a security object for use in authenticating a user to access ~~securing~~ an item, comprising:

means for receiving security object data;

means for setting one or more attributes associated with the security object data, wherein the one or more attributes include a user designation of a security object type; and

means for encapsulating, within the security object, the security object data and the one or more attributes with one or more methods, wherein the security object is used to authenticate the user by validating an identity of the user using at least one of the one or more methods encapsulated within the security object ~~control access to secured contents~~.

36. (Original) The apparatus of claim 35, means for obtaining one or more methods from a security object class.

37. (Original) The apparatus of claim 35, wherein the one or more methods operate on the security object data and one or more attributes.

38. (Currently amended) The apparatus of claim 35, wherein the one or more methods operate on the security object data and input data provided by the user and passed to the security object to authenticate the user to access the item.

39. (Original) The apparatus of claim 35, wherein the security object data is one of textual data, audio data, graphical data, and biometric data.

40. (Original) The apparatus of claim 35, wherein the security object type is one of a single use security object, a group security object, a timed security object, a concurrent multi-user security object, a security object throttle, a translated password security object, a security object augmented by a at least one of a CPU identifier, a CPU speed and a system configuration, a Wave file or MP3 security object, an image file security object, a security object augmented by a location of the user, a security object augmented by a current window and/or pointer position, a security object augmented by an IP address, a security object augmented by a screen background characteristic, a security object augmented by a personal identification number and one of a speed of a card swipe and a number of times of a card swipe, a security object augmented by a mobile telephone ring or mobile telephone identification number, a security object augmented by a caller identification of the user, and a security object augmented by an environmental condition.

41. (Currently amended) The apparatus of claim 35, further comprising:

means for providing the security object to a security system, wherein the security system is ~~not made aware of the security object type~~ a hardware data processing system that stores the security object and associates the security object with a user identification so that the security object may be retrieved when the user enters their identification in order to gain access to the item.

42. (Currently amended) The apparatus of claim 41, wherein the security system invokes the security object in response to a request for access to the item by the user.

43. (Original) The apparatus of claim 18, further comprising means for storing the security object data on an electronic medium in a device with data transmission capability.

44. (Original) The apparatus of claim 43, wherein the device is a portable device.

45. (Original) The apparatus of claim 44, wherein the portable device is one of a keychain, a portable MP3 player, a mobile telephone, a pager, an electronic wrist watch, a remote control, a garage door transmitter, a keyless entry device for a vehicle, a smartcard, and a magnetic stripe card.

46. (Original) The apparatus of claim 41, wherein the security object contains a partial set of methods and wherein the security system contains a complementary set of methods.

47. (Original) The apparatus of claim 35, wherein the security object requires hardware assistance for authentication of input data passed to the security object.

48. (Original) The apparatus of claim 35, wherein the security object data is received from a client apparatus.

49. (Original) The apparatus of claim 35, wherein the security object data is received from a user via a user interface.

50. (Original) The apparatus of claim 49, wherein the user interface is a security object foundry application resident on a computing device.

51. (Original) The apparatus of claim 49, wherein the user interface is an interface transmitted from a server apparatus to a client apparatus.

52. (Currently amended) A method of securing contents, comprising:

receiving a request for access to the contents, the request including input data from a user;

in response to receiving the request for access, retrieving ~~the a user defined~~ a user defined security object previously defined by the user;

applying the user defined security object to the input data from the user; and

controlling access to the contents based on the application of the user defined security object to the input data using a method within the user defined security object.